Cloud Edition and Myriad Series SIP Phones

Deployment Guide with Open SIP PBXs

Alcatel Lucent Enterprise Communication Device Business

Web: www.aledevice.com; www.al-enterprise.com

Email: sales.alesip@al-enterprise.com

Legal notice

Disclaimer

While efforts were made to verify the completeness and accuracy of the information contained in this documentation, this document is provided "as is". To get more accurate content concerning Cross Compatibilities, Product Limits, Software Policy and Feature Lists, please refer to the accurate documents published on the Business Partner Web Site.

In the interest of continued product development, ALE International reserves the right to make improvements to this documentation and the products it describes at any time, without notice or obligation.

The CE mark indicates that this product conforms to the following Council Directives:

- 2014/53/EU for radio equipment
- 2014/35/EU and 2014/30/EU for non radio equipment (including wired Telecom Terminal Equipment)
- 2014/34/EU for ATEX equipment
- 2011/65/EU (RoHS)
- 2012/19/EU (WEEE)

Contents

1. Introduction

This document describes the deployment of ALE Cloud Edition and Myriad Series SIP DeskPhone sets with Open SIP server.

The following sets are covered:

Alcatel-Lucent Enterprise 8008 Cloud Edition DeskPhone (8008 CE)

Alcatel-Lucent Enterprise 8008G Cloud Edition DeskPhone (8008G CE)

Alcatel-Lucent Enterprise 8018 Cloud Edition DeskPhone (8018 CE)

Alcatel-Lucent Enterprise 8058s Cloud Edition DeskPhone (8058s CE)

Alcatel-Lucent Enterprise 8068s Cloud Edition DeskPhone (8068s CE)

Alcatel-Lucent Enterprise 8078s Cloud Edition DeskPhone (8078s CE)

Alcatel-Lucent Enterprise Myriad Series DeskPhone (M3)

Alcatel-Lucent Enterprise Myriad Series DeskPhone (M5)

Alcatel-Lucent Enterprise Myriad Series DeskPhone (M7)

ALE Cloud Edition/Myriad Series SIP phones deployment guide provides general guidance on setting up phone network, provisioning and managing phones.

This guide is not intended for end users, but for administrator with experience in networking who understand the basis of open SIP networks and VoIP endpoint environments.

As an administrator, you can do the following with this guide:

- Set up a VoIP network and provisioning server.
- Provision the phones with features and settings.
- Troubleshoot, upgrade and maintain phones.

Glossary

ALE	Alcatel-Lucent Enterprise
CE	Cloud Edition
DHCP	Dynamic Host Configuration Protocol
EDS	Easy Deployment Service
FQDN	Fully Qualified Domain Name
HTTP/HTTPS	Hypertext Transfer Protocol/Hypertext Transfer Protocol Secure
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
M Series	Myriad Series
MMI	Man Machine Interface
PoE	Power over Ethernet
RAM	Random Access Memory
SIP	Session Initiation Protocol
SSH	Secure Shell
URL	Uniform Resource Locator
USB	Universal Serial Bus
VCI	Vendor Class Identifier
WBM	Web Based Management
WAN	Wide Area Network

2. Accessing Phone Set Information

This chapter describes where ALE Sip phones fit in your network, and provides basic initialization instructions of SIP phones.

2.1 Requirements

In order to perform as SIP endpoints in your network successfully, you need the following in deployments:

- ALE CE/M series SIP phones with compatible firmware.
- A working IP network.
- An active SIP call server.
- A text editor, such as Notepad++, to create and edit configuration files.

2.2 Verifying Startup

The phone begins the initialization process by following steps after connected the power and network:

1) The power LED indicator glows blue.

2) The message “Welcome” appears on the phone screen when the IP phone starts up.

3) For M series phone, press OK key on navigator keypad to check the phone’s status quickly. The phone’s information will display on the screen like the valid IP address, MAC address, firmware version, and more.

For CE series phone, go to “Settings” menu press “Network” softkey to check the IP parameters, press “Version” softkey to check the phone’s firmware version.

3. Phone set provisioning overview

This chapter gives general indication on the parameters that must be provisioned to start a set, the different ways to provision these parameters, and the priority rules between them.

Basically, parameters that must be provisioned are:

- IP parameters (IP address, netmask and router IP address)
- SIP account parameters (SIP server address, register name, username, password)
- Provision URL when SIP parameters are provisioned via SIP configuration files downloaded from a provisioning server

The different ways to provision these parameters are:

- IP parameters:
  - Statically via MMI: see *Configuring IP parameters via MMI* on page 16
  - Dynamically via DHCP

- SIP account parameters:

Manually:

  - Via MMI: see Configuring SIP account parameters via MMI o Via WBM: see Configuring SIP account parameters via WBM

Automatically

- Via SIP configuration files downloaded from a provisioning server: see Building a SIP configuration file
- Provision URL (required only in case of initialization with SIP configuration files)

Manually:

o Via MMI: see Configuring the provisioning server URL via MMI

o Via WBM: see Configuring the provisioning server URL via WBM

Automatically:

o Via DHCP: see DHCP configuration for download path of SIP configuration file

o Via PnP

o Via EDS server

o Via EPS server

The method you use depends on how many phones need to be deployed and what features and settings to be configured. We recommend using manual provisioning as your primary provisioning method when just need several phones for testing.

	IP Parameters	**SIP parameters**	**Auto Provision URL**
Scenario 1	MMI	MMI	N/A
Scenario 2	DHCP	WBM	N/A
Scenario 3	DHCP	Config file	WBM
Scenario 4	DHCP	Config file	DHCP
Scenario 5	DHCP	Config file	PnP Multicast
Scenario 6	DHCP	Config file	EDS
Scenario 7	DHCP	Config file	EPS

Commissioning phone sets on page 11 details four possible scenarios

3.1 Provisioning method priority

A priority order is defined between the different provisioning methods: settings you make using a higher priority provisioning method will override settings made using a lower priority method.

The priority order for setting provisioning is:

1) Settings received from the config file which is deployed by provisioning server

2) Settings received from the DHCP server

3) Settings configured locally via MMI or WBM

4) Factory default settings

For the Auto provision URL configuration, the priority is the following:

1) Auto provision URL received from DHCP
2) Auto provision URL received from PnP
3) Auto provision URL configured via MMI or WBM
4) Auto provision URL received from EDS

3.2 Commissioning Phone Sets

Scenario 1: Configuring IP and SIP parameters via MMI

Scenario 1 describes the commissioning of a set on the LAN with IP static initialization (**no DHCP server**) and without SIP configuration files (**no provisioning server**). In this scenario, all the configuration is performed via the set MMI.

Before beginning: you must know the following:

- IP parameters of the set (IP address, netmask, router IP address)
- SIP parameters: SIP call server information (IP addressing, port, authentication)

To commission the set:

1) Configure the phone set on the SIP call server as needed according to the SIP server documentation

2) Connect the set: see *Connecting the phone set to the customer network*

3) Access the phone set user interface (MMI) and configure the following:

- Change the initialization mode from **Dynamic** (default mode) to **Static**: see: *Configuring IP parameters via MMI*
- Configure the IP parameters of the phone set: see: *Configuring IP parameters via MMI*
- Configure SIP parameters (via a SIP account): see: *Configuring SIP account parameters via MMI*

4) Save all configuration and then reboot the phone set.

After startup, the set automatically begins initialization process. After the last initialization step, the set registers to the SIP server.

Scenario 2: IP dynamic configuration on LAN, no SIP configuration file

Scenario 2 describes the commissioning of a set on the LAN with IP dynamic initialization (provision of standard IP parameters by DHCP server) and without SIP configuration files (no provisioning server). In this scenario, the set gets its IP parameters from the DHCP server and SIP parameters are configured manually via WBM.

Before beginning: you must know the following:

- SIP parameters: SIP call server information (IP addressing, domain, authentication)

Prerequisites:

- A DHCP is operational on the LAN (no specific configuration required): see *Setting up a DHCP server* on page 23

To commission the set:

1) Configure the phone set on the SIP call server as needed according to the SIP server documentation
2) Connect the set
3) Read the IP address on the phone set display
4) Access the phone set configuration via WBM. Input https://ipaddress in browser to access and then login with “admin” (password is 123456 by default).
5) Configure SIP parameters by going to **Accounts -> Basic.**

After startup, the set automatically begins initialization process. After the last initialization step, the set registers to the SIP server.

Scenario 3: IP dynamic configuration on LAN with SIP configuration file setting by WBM

Scenario 3 describes the commissioning of a set on the LAN with IP dynamic initialization (provision of standard IP parameters by DHCP server) and with SIP configuration file which will be downloaded during set initialization from a provisioning server, whose URL is configured via WBM.

Before beginning: you must know the following:

- SIP parameters: SIP call server information (IP addressing, domain, authentication): this information is required to build the configuration file

Prerequisites:

- The phone set must initialize in dynamic mode (default mode)
- A DHCP is operational on the LAN and configured to provide standard IP parameters (IP address, DNS, NTP etc.): see *Setting up a DHCP server*
- A provisioning server is operational on the LAN: see *Setting up a provisioning server*

To commission the set:

1) Configure the phone set on the SIP call server as needed according to the SIP server documentation
2) Create and configure the SIP configuration file: see: *Building a SIP configuration file*
3) Deploy the SIP configuration file in the provisioning server relative directory
4) Connect the set: see *Connecting the phone set to the customer network*
5) Read the IP address on the phone set display
6) Access the phone set configuration via WBM. Input https://ipaddress in browser to access the phone and then login with “admin” (password is 123456 by default). see *Configuring SIP account parameters via WBM* for detail.
7) Configure Auto Provision URL parameters by going to **Auto Provision -> Basic.**

8) Save all settings and then reboot the phone.

After startup, the set automatically begins initialization process. After the last initialization step, the set registers to the SIP server.

Scenario 4: IP dynamic configuration on LAN with SIP configuration file via DHCP

Scenario 4 describes the commissioning of a set on the LAN with IP dynamic initialization (provision of standard IP parameters by DHCP server) and with SIP configuration file which will be downloaded during set initialization from a provisioning server, whose URL is provided by the DHCP server: this requires a specific configuration on the DHCP server. In this scenario, the set starts without any manual operation via MMI or WBM.

Before beginning: you must know the following:

- SIP parameters: SIP call server information (IP addressing, domain, authentication): this information is required to build the configuration file

Prerequisites:

- The phone set must initialize in dynamic mode (default mode)
- A DHCP is operational on the LAN and configured to provide the URL of the provisioning server (Auto Provision URL): see *Setting up a DHCP server* and *DHCP configuration for download path of SIP configuration files*
- A provisioning server is operational on the LAN: see *Setting up a provisioning server*

To commission the set:

1) Configure the phone set on the SIP call server as needed according to the SIP server documentation

2) Create and configure the SIP configuration file: see: *Building a SIP configuration file*

3) Deploy the SIP configuration file in the provisioning server relative directory

4) Connect the set: see *Connecting the phone set to the customer network*

After startup, the set automatically begins initialization process. After the last initialization step, the set registers to the SIP server.

Scenario 5: IP dynamic configuration on LAN with SIP configuration file via PnP

Scenario 5 describes the commissioning of a set on the LAN with IP dynamic initialization (provision of standard IP parameters by DHCP server) and with SIP configuration file which will be downloaded during set initialization from a provisioning server, whose URL is provided by PnP multicast message: In this scenario, the set starts without any manual operation via MMI or WBM (zero touch).

Before beginning: you must know the following:

- SIP parameters: SIP call server information (IP addressing, domain, authentication): this information is required to build the configuration file

Prerequisites:

- The phone set must initialize in dynamic mode (default mode)
- A DHCP is operational on the LAN and configured to provide standard IP parameters (IP address, DNS, NTP etc.): see *Setting up a DHCP server*
- A provisioning server is operational on the LAN: see *Setting up a provisioning server*

- A PnP server: generally, it is provided by SIP server.

To commission the set:

1) Configure the phone set on the SIP call server as needed according to the SIP server documentation
2) Create and configure the SIP configuration file: see: *Building a SIP configuration file*
3) Deploy the SIP configuration file in the provisioning server relative directory
4) Connect the set: see *Connecting the phone set to the customer network*
5) After startup, the set automatically begins initialization process. After the last initialization step, the set registers to the SIP server.

Scenario 6: IP dynamic configuration on LAN with SIP configuration file via EDS (ALE redirect provision serves

ALE CE/M DeskPhones support Zero Touch Deployment using ALE Easy Deployment Server (EDS). You can contact the ALE EDS administrator account.eds@al-enterprise.com for more information. You can connect to https://admin.eds.al-enterprise.com/register to sign-up for a free EDS account.

ALE EDS is a server side service that helps ALE CE/M series DeskPhone sets to connect to the provisioning server on first startup. The service is deployed on the Internet Cloud.

The EDS server allows to provision sets with the Auto Provision URL and certificates, allowing them to initialize from the WAN without requiring a specific configuration of the DHCP server.

When the set starts in dynamic mode and no provisioning server URL is configured via MMI or received from DHCP/PnP, it tries to connect to the ALE EDS server, whose address is hard-coded in its software. The server verifies the set's MAC address, and searches a profile for the set in the database.

The provisioning server URL and certificate relative URL are provided in the profile. The set downloads certificate, connects to the provisioning server via this URL, and downloads its SIP configuration file.

Note:

Auto-provisioning with EDS does not apply to phone sets initializing in static mode.

Scenario 6 describes the commissioning of a set on the WAN with IP dynamic initialization (provision of standard IP parameters by DHCP server) and with SIP configuration files which will be downloaded during set initialization from a provisioning server, whose URL is provided by the EDS server: this requires a specific configuration on the EDS server. In this scenario, the set starts without any manual operation via MMI or WBM (zero touch).

Before beginning: you must know the following:

SIP parameters: SIP call server information (IP addressing, domain, authentication): this information is required to build the configuration file

Prerequisites:

- The phone set can reach the WAN
- The phone set must initialize in dynamic mode (default mode)
- A DHCP is operational on the LAN (no specific configuration required)
- A provisioning server is operational on the WAN or Cloud: see Setting up a provisioning server
- A profile associated to the phone MAC address has been created on the EDS server to auto provision URL and certificate relative URL

To commission the set:

1) Configure the phone set on the SIP call server as needed according to the SIP server documentation

2) Create and configure the SIP configuration file: see: Building a SIP configuration file

3) Deploy the SIP configuration file in the provisioning server relative directory

4) Connect the set: see Connecting the phone set to the customer network

After startup, the set automatically begins initialization process. After the last initialization step, the set registers to the SIP server.

Scenario 7: IP dynamic configuration on LAN with SIP configuration file via EPS (ALE provision server)

ALE CE/M series SIP DeskPhone sets support zero touch deployment by the Easy Provision Service (EPS). You can refer to the EPS User Manual for more detailed

Scenario 7 describes the commissioning of a set on the LAN with IP dynamic initialization (provision of standard IP parameters by DHCP server) and with SIP configuration files which will be downloaded during set initialization from a provisioning server, whose URL is provided by the EPS server: this requires a EPS tool installed in the LAN. In this scenario, the set starts without any manual operation via MMI or WBM (zero touch).

Before beginning: you must know the following:

- SIP parameters: SIP call server information (IP addressing, domain, authentication): this information is required to build the configuration file

Prerequisites:

- The phone set must initialize in dynamic mode (default mode)
- A DHCP is operational on the LAN (no specific configuration required)
- A EPS tool is installed in LAN.

To commission the set:

1) Configure the phone set on the SIP call server as needed according to the SIP server documentation.

2) Create and configure the SIP configuration file via EPS with EPS use manual help.

3) Connect the set: see *Connecting the phone set to the customer network*

4) After startup, the set automatically begins initialization process. After the last initialization step, the set registers to the SIP server.

3.3 Connecting the phone set to the customer network

To connect the phone set to the customer network:

- If the phone set is powered by PoE:
  1) Plug the RJ45 cable into the set LAN connector
  2) Connect the RJ45 cable to the customer network via a PoE hub/switch (IEEE802.3af compliant)
- If the phone set is not powered by PoE, plug the AC/DC external adapter to the set power supply connector (DCSV) and connect the plug to the power supply

Once the phone set is connected and powered up, it automatically starts initializing.

The phone set begins the initialization process by following steps after connected the power and network:

For ALE CE phone:

1) The call and message LEDs indicators glow blue.

2) The message “Welcome” appears on the phone screen when the phone set starts up.

3) The main phone screen displays the following:

4) Firmware version on the top of the screen

5) Each initialization step, from step 1 to 5.

6) Press right key on navigator keypad to enter the settings menu. Then you can check the phone screen displays the valid IP address, MAC address, phone configuration, firmware version, help for Navigator key using, and so o

For ALE Myriad phone:

1) The navigator key pad and softkey LEDs indicators glow blue.
2) The message “Welcome” appears on the phone screen when the phone set starts up.
3) Press OK key on navigator keypad or press “Menu” softkey to enter the “Status” page. Then you can check the phone screen displays the valid IP address, MAC address, firmware version. You can select “More” to check more detailed information like Network, Phone’s software and hardware info and accounts register status.

4. Configuring phone sets

4.1 Configuring IP parameters via MMI

The CE setting menu of the MMI can be accessed when the phone is started:

1) Go to “Admin” setting on CE, enter the admin password (the default admin password for the phone out of box is 123456).

2) Press the softkeys **IP param** > **IP Config** > **IPv4 settings** to access the IP parameters setting page. This page allows to select the initialization mode (The default DHCP mode is dynamic) and to configure network parameters if static mode is selected.

3) Press the softkey next to **IPv4 mode** to switch to **Static.** *This step is optional just when select Static mode*

4) Complete the set IP parameters:

- IP: enter the set IP address
- S/net: enter the IP subnet mask
- Router: enter the default router IP address

Note: This step is optional just when select Static mode.

Note: Non-alphanumeric character input instructions:

- 8008G CE & 8008 CE & 8018 CE: Press the '123<>abc' soft key to switch to non-numeric input mode.
- 8058s CE & 8068s CE & 8078s CE: long Press the “i” key on the phone to switch to non-numeric input mode.
- Special characters ：

Press * key for: %$/&()[]=*

press # key for: @#

press 0 key for: +.,;:\?!0

5) Press the OK key to save modifications
6) Press release key to exit the settings menu.

The set automatically reboots to take these settings changes into account.

The M setting menu of the MMI can be accessed when the phone is started:

1) Go to “Advanced Settings” setting, enter the admin password (the default admin password for the phone out of box is 123456).
2) Go to Network > IP Stack to access the IP stack setting page. This page allows to select the running stack mode, IPv4 is by default.

3) Go to Network > IP Config > IPv4 Settings to access the IP parameters setting page. This page allows to select the initialization mode (The default DHCP mode is dynamic) and to configure network parameters if static mode is selected.

   Note: if select IPv6 in step2, then go to IPv6 settings page to set up IP parameters.

4) Press the navigator keys to IPv4 mode to switch to Static. This step is optional just when select Static mode.

5) Complete the set IP parameters:

- **IP**: enter the set IP address
- **S/net**: enter the IP subnet mask
- **Router**: enter the default router IP address

  Note: This step is optional just when select Static mode.

6) Press the OK key to save modifications

7) Press release key to exit the settings menu.

   The set automatically reboots to take these settings changes into account.

4.2 Configuring the provisioning server URL via MMI

The CE setting menu of the MMI can be accessed when the phone is started:

1) Go to “Admin” setting on CE, enter the admin password (the default admin password for the phone out of box is 123456).

2) Press the softkeys **DM** to access the provision server url parameters setting page.

3) Press the **OK** key to save modifications

4) Press release key to exit the settings menu.

The set automatically reboots to take these settings changes into account.

The M setting menu of the MMI can be accessed when the phone is started:

1) Go to “Advanced Menu” setting, enter the admin password (the default admin password for the phone out of box is 123456).

2) Go to **Auto Provision>URL** to access the provision server url parameters setting page. Then input right provision URL.

3) Note: you can also input **User Name** and **Password** for HTTP digest authentication method.

4) Press the **OK** key to save modifications

5) Press release key to exit the settings menu.

The set automatically reboots to take these settings changes into account.

4.3 Configuring SIP account parameters via MMI

The CE setting menu of the MMI can be accessed when the phone is started

1) Go to “Admin” and then enter the admin password (the default admin password for the phone out of box is 123456).

2) Press down key on navigator keypad until the last page and press **Sip servers** softkey.

3) Select a SIP account and configure related SIP server connection parameters.

   Note: Non-alphanumeric character input instructions:

- 8008G CE & 8008 CE & 8018 CE: Press the '123<>abc' soft key to switch to non-numeric input mode.
- 8058s CE & 8068s CE & 8078s CE: long Press the “i” key on the phone to switch to non-numeric input mode.
- Special characters ：

  Press * key for: %$/&()[]=*

  press # key for: @#

  press 0 key for: +.,;:\?!0

4) Press the **OK** key to save modifications.

5) Press release key to exit the settings menu.

6) The set automatically reboots to take these settings changes into account.

The M setting menu of the MMI can be accessed when the phone is started:

1) Go to **“Advanced Menu”** and then enter the admin password (the default admin password for the phone out of box is 123456).

2) Go **“Account”** to access the SIP accounts setting page.

3) Select a SIP account and configure related SIP server connection parameters.

4) Press the **OK** key to save modifications.

5) Press release key to exit the settings menu.

The set automatically reboots to take these settings changes into account.

5. Configuring SIP parameters via WBM

You can configure ALE CE/M series DeskPhone sets via web user interface (WBM) when the phone has started up with proper IP parameters.

1) To find the IP address of the set: for CE phone, in the set user interface (MMI), select **Settings** > **Network** and read the IP address; for M phone, press OK button find the IP address.

2) In a web browser, enter the URL: https://[IP address], for example https://192.168.0.10

3) You are prompted to enter login/password:

4) login: enter **admin**

5) password: enter the password (default password is 123456)

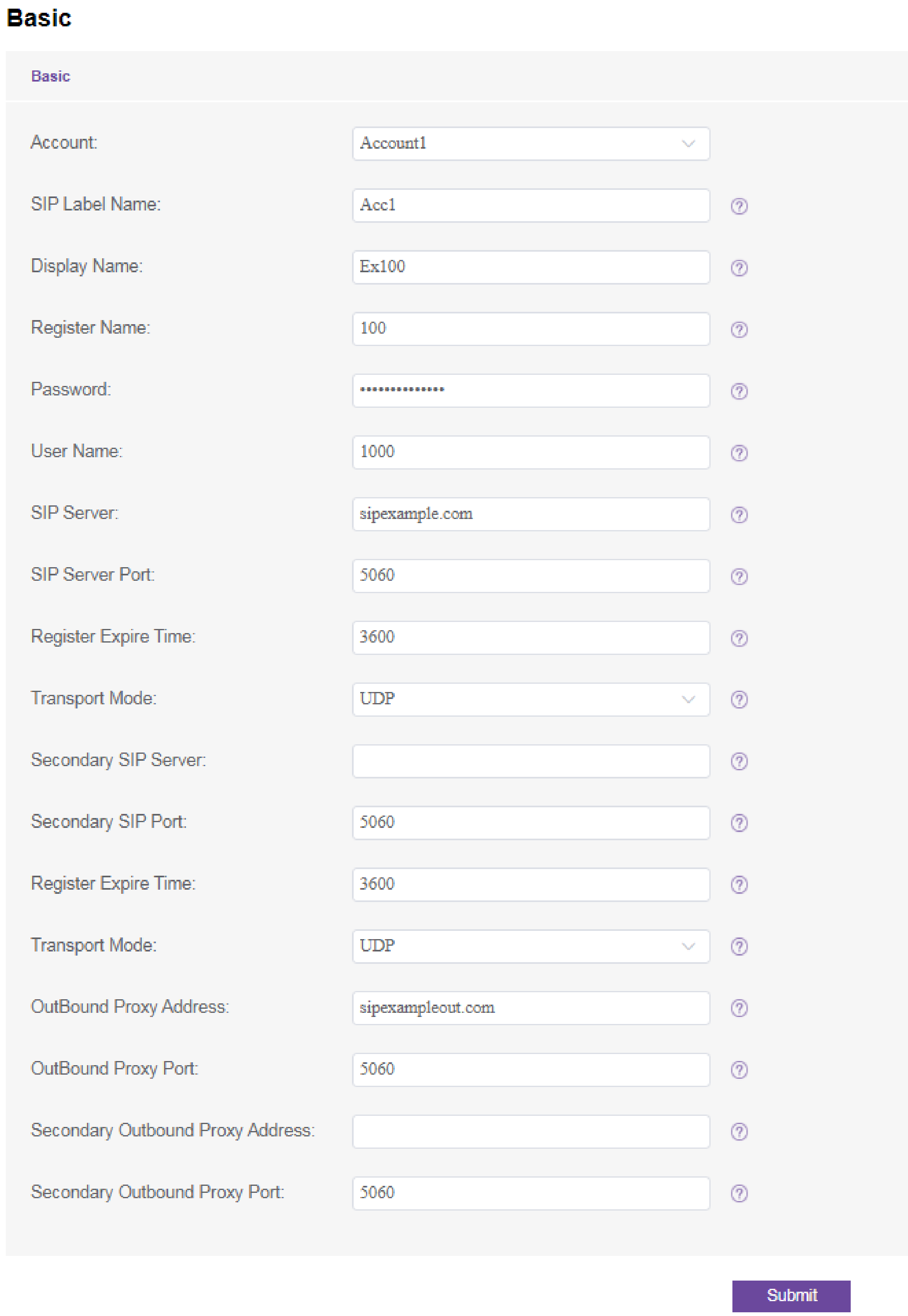
6) Click **Login**

7) **Go to Accounts -> Basic to access the SIP accounts setting page.**

8) Select a SIP account and configure related SIP server connection parameters.

9) Click **“submit”** to save the modifications.

The set will take these settings changes into account.

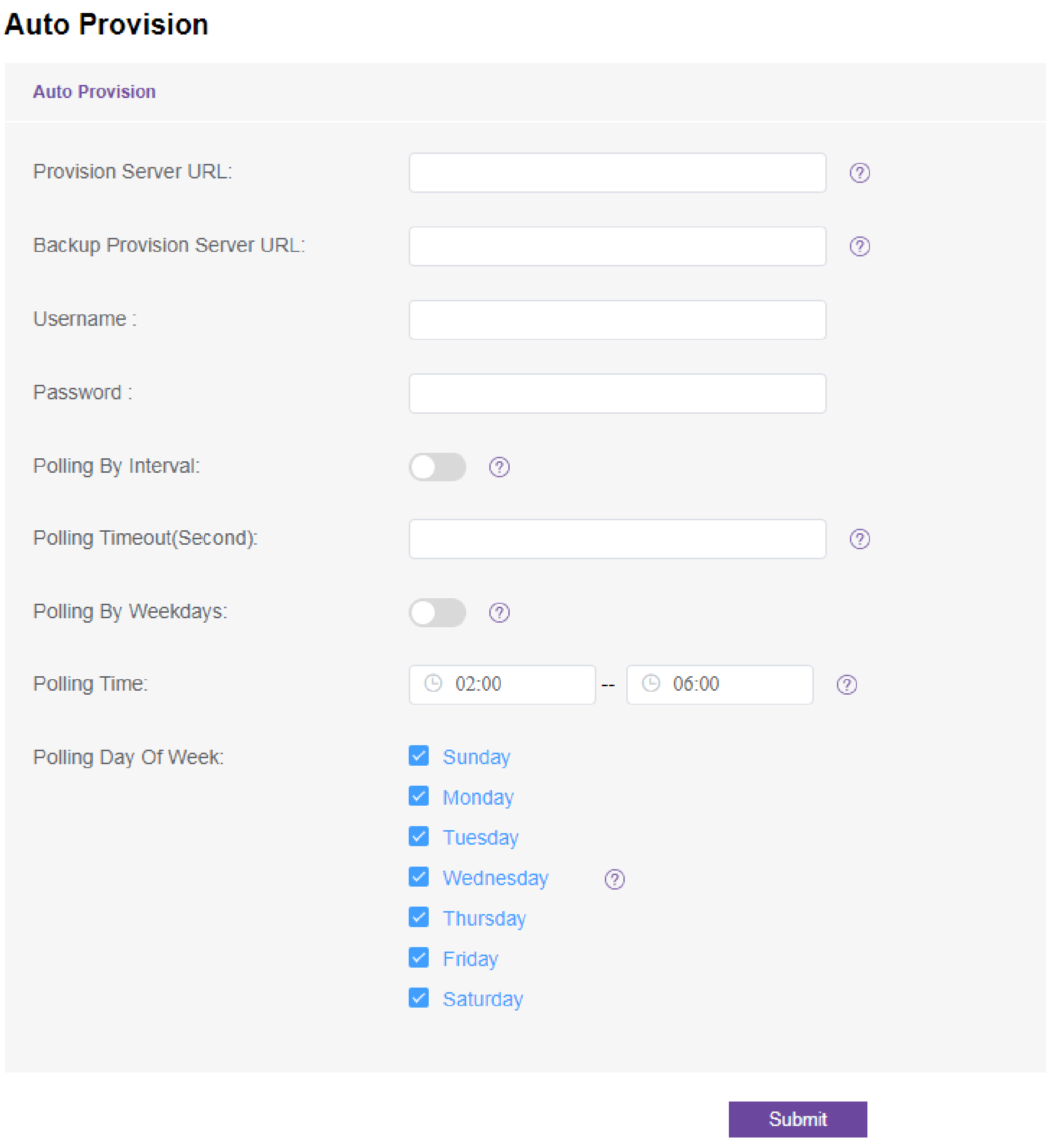


5.1 Configuring the provisioning server via WBM

You can configure ALE CE/M series DeskPhone sets via web user interface (WBM) when the phone has started up with proper IP parameters.

1) To find the IP address of the set: for CE phone, in the set user interface (MMI), select Settings > Network and read the IP address; for M phone, press OK button find the IP address.

2) In a web browser, enter the URL: https://[IP address], for example https:// 192.168.0.10
3) You are prompted to enter login/password:
   - login: enter **admin**
   - password: enter the password (default password is 123456)
4) Click Login
5) Go to Settings > Auto Provision to access the Provision Server URL setting page.
6) Fill in Provision URL.
7) You can also fill the User Name and Password for HTTP digest authentication method.
8) Click "submit" to save the modifications.
9) The set will take these settings changes into account.



5.2 Setting up a DHCP server

This chapter details the configuration of the DHCP server to be performed when ALE CE/M series DeskPhone sets initialize in dynamic mode.

The DHCP can be used to provide standard IP parameters only or standard IP parameters and the Auto Provision URL. When the Auto Provision URL is not provisioned by the DHCP server, no specific configuration is required on the DHCP server: only standard IP parameters are required.

You can skip this section if ALE CE/M series DeskPhone sets initialize in static mode.

If configured for dynamic IP address, the CE/M phone retrieves its network configuration parameters from the DHCP server during step 3 of its initialization.

DHCP option configuration for IPv4 details the list of DHCP options supported by ALE *CE/*M series DeskPhone sets.

DHCP configuration for download path of SIP configuration files describes how to configure the download path of SIP configuration files on the DHCP server.

Note:

Configuring the download path is not required when auto-provisioning with PnP/EDS/EPS is used.

5.3 DHCP option configuration for IPv4

The following table lists common DHCP options for IPv4 supported by ALE CE/M series DeskPhone sets.

Parameter	DHCP option	Description
Subnet Mask	1	Specify the client's subnet mask
Router	3	Specify a list of IP addresses for routers on the client's subnet
Domain Name Server	6	Specify a list of domain name servers available to the client
Host Name	12	Specify the name of the client. (sent by default)
Domain Server	15	Specify the domain name that client should use when resolving hostnames via DNS
Network Time Protocol Servers	42	Specify a list of NTP servers available to the client by IP address
Vendor-Specific Information	43	Identify the vendor-specific information
Vendor Class Identifier	60	Identify the vendor type (ictouch.0)

Parameter	DHCP option	Description
Auto Provision server	66	Identify one Auto Provision URL
option 43 > sub-option 67	67	Sub-option of Option 43, to define the auto provision path
Default user class	77	ictouch.class0

table 7.1: DHCP Options

5.4 DHCP configuration for download path of SIP configuration files

The table below describes the different possibilities for the configuration on the DHCP server of the download path for SIP configuration files.

You can ignore this section if auto-provisioning with EDS which is ALE redirect provision server is used.

	8008 CE/ 8008G CE	8018 CE	8058s CE	8068s CE	8078s CE	M3	M5	M7
VCI (dhcp option 60) (not modifiable)	ictouch.0	ictouch.0	ictouch.0	ictouch.0	ictouch.0	ictouch.0	ictouch.0	ictouch.0
Default user class (option 77) (not sent by default)	ictouch. class0	ictouch. class0	ictouch. class0	ictouch. class0	ictouch. class0	ictouch. class0	ictouch. class0	ictouch. class0
Default hostname (option 12) (sent by default)	8008-XXYYZZ	8018-XXYYZZ	8058s-XXYYZZ	8068s-XXYYZZ	8078s- XXYYZZ	M3- XXYYZZ	M5- XXYYZZ	M7- XXYYZZ

table 7.2: Configuration for DHCP Option 12, Option 60 and Option 77

Option 66	Option 43 > sub option 67 (full path)	Option 43 > sub option 67 (relative path)	Download path
		√	Invalid combination
√			https://option 66/
√		√	https://option 66/sub-option 67/
	√		Sub-option 67

table 7.2: Configuration of download path on DHCP

Option 66	Option 43 > sub option 67 (full path)	Option 43 > sub option 67 (relative path)	Download path
192.168.2.2/ale/config			https://192.168.2.2/ale/config
192.168.2.2		ale/config	https://192.168.2.2/ale/config
	192.168.2.2/ale/config		https://192.168.2.2/ale/config
	**http://192.168.2.2/ale/config		http://192.168.2.2/ale/config

table 7.3: Configuration example for download path

** Recommend way

6. Setting up a provisioning server

6.1 Provisioning server setup overview

A provisioning server is necessary when SIP configuration files are used.

You can skip this section if ALE CE/M series DeskPhone sets initialize without SIP configuration files

ALE CE/M series DeskPhone sets support the following transport protocols for provisioning:

The HTTP/HTTPS provisioning server can be set up on the local LAN. Use the following procedure as a recommendation if this is your first provisioning server setup.

To set up the provisioning environment:

1) Install an HTTP/HTTPS server application or locate a suitable existing server.

2) Create an account and home directory.

3) Set security permissions for the account.

Once the setup has been completed, create the SIP configuration files required for set commissioning (see: Building a SIP configuration file), and copy them in the HTTP/HTTPS provisioning server relative directory.

If the CE/M phone has retrieved a DM/Provision URL from the DHCP server, it downloads the configuration file from the provisioning server during step 4 of its initialization.

Note:

The DM/Provision URL which is configured in the DHCP server corresponds to the path of the SIP configuration files stored on the provisioning server.

6.2 HTTP server setup

Configure a Windows server system (or virtual system) to set up an Apache web server with following standard steps. When the Apache web server has been successfully installed, create a directory on this server to store the SIP configuration files or firmware binary files, and get the download URL for set commissioning.

To set up an Apache HTTP server, go to *www.apache.org* and download the last version of Apache web server. You can find detailed steps about how to set up Apache server through world wide web. It is recommended to set up this kind of server if you are one of IT administrator. Generally, we strong recommend setting up one HTTP serve with some software tool like HFS or MobaXterm when you just establish one simple provision environment. Here we take MobaXterm for example to show how to setup one HTTP server.

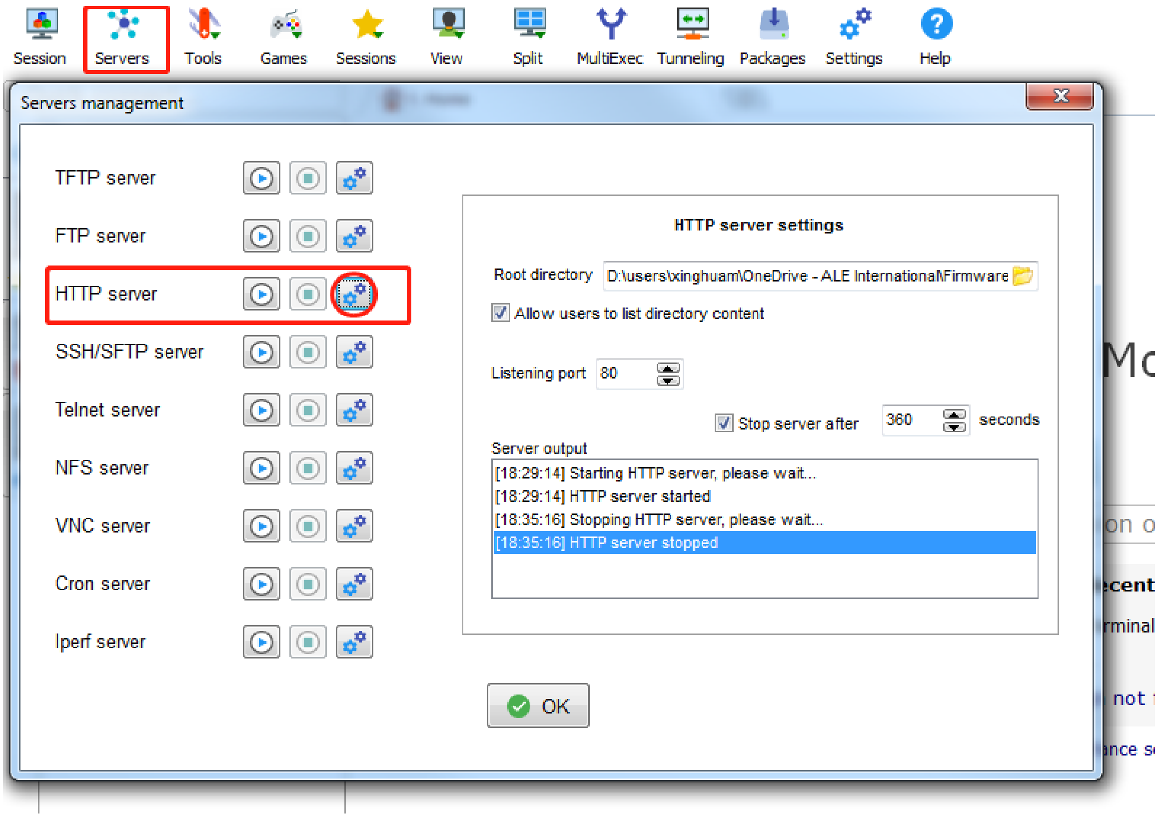
1) **Step1:** Preparing the config file: config.{mac-address}.xml

In the config file the following contents should be included at least:

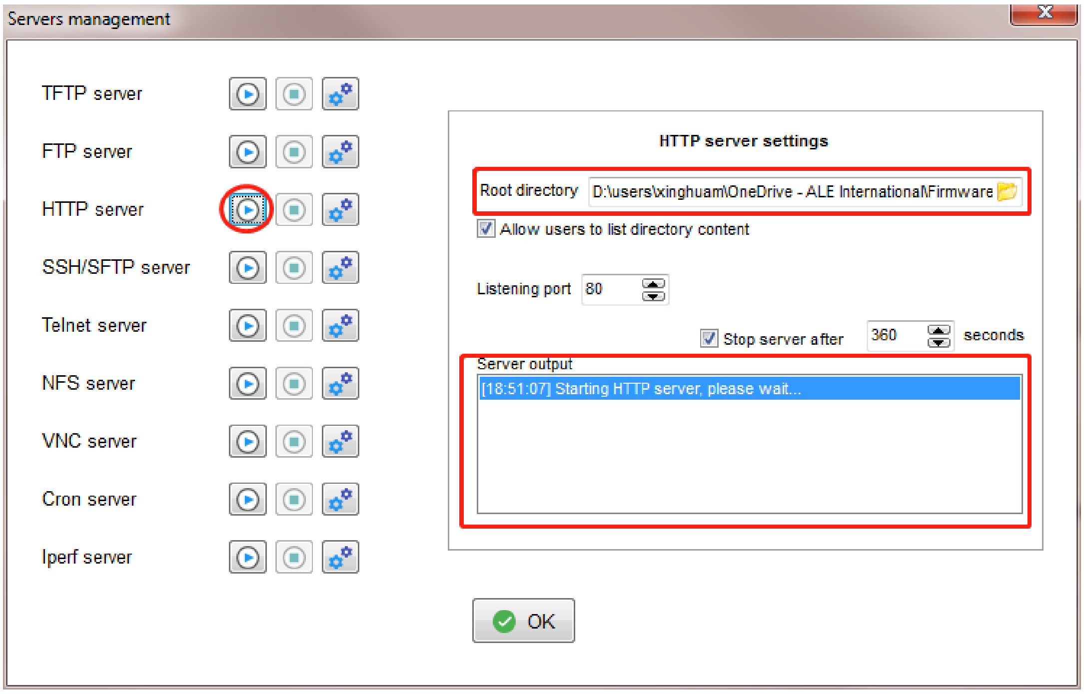

```xml
<?xml version="1.0" encoding="UTF-8" ?>
<settings>
<setting id="SIPServer1Address" value="TestSipDomain.sipserver.com" override="true"/>
<setting id="SIPGroup1DeviceUri" value="Testnumber" override="true"/>
<setting id="SIPGroup1AuthenticationPassword" value="TestSipPassword" override="true"/>
<setting id="DmAdminPasswd" value="000000" override="true"/>
</settings>
```

Note: For details on the file structure, see: SIP configuration file templates.

2) Step2: Installed the MobaXterm tool on your PC.
3) Step3: Open the tool and go to “Servers → HTTP server → “setting” (red circle)



4) Step 4: Copy the path which you saved config file on you PC in “Root directory” and then press  to run the HTTP server on your PC.



Note: you will see the “HTTP server started” log in “Server output” box.

5) Step 5: Check the IP address of your PC, “135.251.222.150” for example.
6) Step 6: login the phone by web with default password “123456”.

Then go to Settings---> Auto Provision--->Provision URL, then fill the path in. The path is equal to the value of blue box field shown in the image1.

7) Step 7: Press “Submit” to take the url setting into account.
8) Step 8: The phone will restart and then download the config file.

When the phone is starting up its admin password will be “000000” which is defined in config file with sentence “<setting id="DmAdminPasswd" value="000000" override="true"/>”

You can define the password by modify the value.

6.3 Building a SIP configuration file

Before beginning, you must have the following:

- The MAC address of the phone set required for the name of the SIP configuration file (config. {mac address of the phone set}.xml, for example config.00809fe7021e.xml)
- A text editor, such as Notepad++, to create and edit configuration file

Build the SIP configuration file required for set commissioning:

1) Install an HTTP server application or locate a suitable existing server.

For details on the file structure, name and minimum settings, see: *SIP configuration file templates*.

2) Complete the SIP configuration file according to your needs.

For details on the available settings, see: *Description of the SIP Settings in configuration file* on page 36.

Once creation is completed, copy the SIP configuration file in the HTTP/HTTPS provisioning server relative directory.

7. Upgrading the firmware

This chapter details the firmware upgrade of ALE CE/M series DeskPhone sets. You can have the binary by accessing http://www.aledevice.com/site/download

7.1 Upgrading by WBM

1) Put the new firmware version on your local PC

2) Connect to the set WBM (as explained in *Configuring IP parameters and SIP account parameters via WBM*) and go to: **Maintenance** > **Binary Update**

3) Click **Select**

4) Select the binary file:

For CE phone, it's depending on the phone types:

- Sip8008N is for 8008 CE and 8008G CW
- Sip8018N is for 8018 CE
- Sip80x8s is for 8058s CE/8068s CE/8078s CE since 1.53

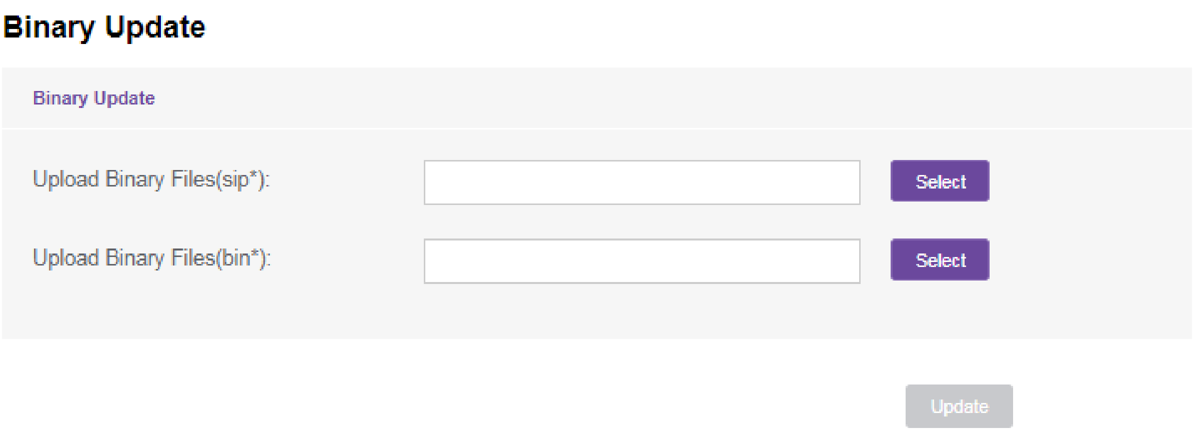
Note: if the CE phone software version is lower than 1.53.13, it's 1.52.04 for example, then you need rename sip80x8s according to the phone model type. For example, if you want to upgrade one 8058s CE phone with software version 1.52.04 to 1.53.31, you should rename sip80x8s to sip8058s firstly. When you want to upgrade one 8058s CE phone from 1.53.13 to 1.53.31, just need select sip80x8s.

For Myriad phone:

- bin9000N
- sip9000N

5) Click Update

After download, the phone installs the new binary and reboots.



7.2 Upgrading by configuration file

You can upgrade the CE/M phone using the SIP provisioning server and SIP configuration with relevant parameters.

CE/M phone can upgrade by downloading firmware binary files from a provisioning server whose URL must be defined in the SIP configuration file (i.e. config.{mac-adress}.`xml`, for example config. 00809fe7021e.xml).

Settings:

```
<setting id="DmEnetcfgUpgradeFile" value="upgrade URL" override="true"/>
```

Description:

Set up the upgrading URL. Put the firmware binary file in the directory of provisioning server, for example the URL could be http://192.168.2.2/ale/firmware. Then this setting should be:

```
<setting id="DmEnetcfgUpgradeFile" value="http://192.168.2.2/ale/firmware" override="true"/>
```

You can trigger an immediate upgrade by resetting manually the ALE CE/M series DeskPhone set, or enable automatic update by adding settings described below in the SIP configuration file.

Automatic update operates in the following way:

- The phone polls for new binary once a day at the time defined by DmAdmcfgUpdateTimeStart
- To prevent all sets from updating at the same time, DmAdmcfgUpdateTimeDelta can be configured so that each set will update at a random time between DmAdmcfgUpdateTimeStart and DmAdmcfgUpdateTimeStart + DmAdmcfgUpdateTimeDelta. In this way, upgrade parameters are the same for all sets, but each sets will update at a different time.
- If the directory contains a different version (older or newer), the set updates with this version
- If no binary file is available on the server, or the version is the same, nothing happens

The following settings for the SIP configuration file template used for the phone upgrade at phone startup (no daily polling for automatic update).

```
<?xml version="1.0" encoding="UTF-8" ?>

<settings>
<setting id="DmAdmcfgUpdateTimeEnable" value="true" override="true"/>
<setting id="SIPServer1Address" value="TestSipDomain.sipserver.com" override="true"/>
<setting id="SIPGroup1DeviceUri" value="Testnumber" override="true"/>
<setting id="DmEnetcfgUpgradeFile" value="http://192.168.2.2/ale/firmware" override="true"/>
</settings>
```

1) Prepare the SIP configuration file and put it on the SIP provisioning server
2) Put the firmware binary on the SIP provisioning server
3) Set Provision URL in the phone by WBM or by MMI which are introduced in Chapter 4.
4) Start the phone

   The phone downloads the SIP configuration file and reboots to enter the upgrading process. The phone reboots automatically after finishing the whole upgrading process.

5) When the phone restarts, check that it had been upgraded to the desired version.

8. Troubleshooting

8.1 Activating SSH

Some procedures in the following sections require to connect to the phone set via SSH. By default, SSH is deactivated and must be enabled via WBM, or DmSecucfgSsh parameter in the SIP configuration file of the phone set.

Once SSH is enabled, you can connect as admin by SSH. SSH login is "admin" and password is the same as admin password for MMI and WBM.

8.2 Activating SSH by WBM

1) Connect to the set WBM and go to: **Settings** > **Security** > **SSH**

2) Enable **SSH activation** and click **Apply**

Activating SSH by SIP configuration file

1) Download the target SIP configuration file from the HTTP/HTTPS provisioning server relative directory

2) Edit the SIP configuration file via a text editor

3) Insert or modify the DmSecucfgSsh command line as follows:

```
<setting id="DmSecucfgSsh" value="true" override="true"/>
```

4) Upload the target SIP configuration file to the HTTP/HTTPS provisioning server relative directory

5) Reboot the phone set

8.3 Terminal information check (mandatory)

It is mandatory to provide the terminal information for each issue.

```
$ id full      // To get the hardware & software information

$ config       // To get the phone configuration
```

8.4 Collecting system logs

The following commands allow to collect the system logs of the phones.

```
$  cd /log/
$  ls -l
$  tar cvzf /tmp/syslog.tgz *.*
```

Several types of system logs are stored in the folder /log/:

- Defence.log
- Reset.log
- log.rcS
- pltf.log
- upgrade.log

After executing above commands, you may download the `syslog.tgz` file under `/tmp/` and send to ALE International for further analysis.

8.5 Collecting SIP telephony trace

If the issue is related to SIP telephony, below commands are necessary for debug.

The different trace levels are:

- debug
- emerg
- err (default level)
- info
- notice
- warning

The type of logs collected depends on the level: for example, the `err` level allows to collect only the error logs, whereas the `debug` level allows to collect all logs.

Note:

The `debug` level takes more CPU load and memory usage which has an impact on the phone performance. That's why the level should be set to `debug` only for debug purposes, and should be set back to `err` when there are no more errors or after all the necessary log information has been captured.

To get the SIP general information and status:

```
$ dumpsip            //To show the basic SIP settings

$ dumpTelephony      //To show the SIP telephony status
```

To check and set the trace level and collect the trace of telephony:

$ level	//To show the trace level		
ACTIVITY	LEVEL	SUPPORT	DESTINATION
ApplicationManager	err	file	/var/log/ApplicationManager.log
ictaudio	err	file	/var/log/ictaudio.log
ICTCliGateLite	err	file	/var/log/ICTCliGateLite.log
ictsipua	err	file	/var/log/ictsipua.log
LoggerModule	err	file	/var/log/LoggerModule.log
no_facility	err	file	/var/log/no_facility.log
Platform	err	file	/var/log/Platform.log
SettingsManager	err	file	/var/log/SettingsManager.log
sipmmi	err	file	/var/log/sipmmi.log

Telephony	err	file	/var/log/Telephony.log //location of Telephony log
$ level Telephony debug		//To set the Telephony log to debug level	

8.6 Collecting core dump files after crash issue

If a crash issue is detected, collect the related core dump files as below:

```
$ cd /data/core/

$ ls -l

drwxrwxr-x   2   admin   admin   400       Jul 31   15:20 .

drwxr-xr-x   6   root    root    424       Aug 3    2017 ..

-rw-r--r--   1   root    root    332221    Jul 31 15:20 core.ictbtmgr.gz      //core dump file

-rw-r--r--   1   root    root    177122    Jul  4   2006 core.ictsipua.gz     //core dump file

-rw-r--r--   1   root    root    1335296 Jun     23 10:22 core.sipapp_mgr.gz  //core dump file
```


8.7 Collecting audio trace

To check and set the trace level and collect the trace of audio:

$ level //To show the trace level

ACTIVITY	LEVEL	SUPPORT	DESTINATION	
ApplicationManager	err	file	/var/log/ApplicationManager.log	
ictaudio	err	file	/var/log/ictaudio.log	//location of ictaudio
log	err	file	/var/log/ICTCliGateLite.log	
ICTCliGateLite				
ictsipua	err	file	/var/log/ictsipua.log	
LoggerModule	err	file	/var/log/LoggerModule.log	
no_facility	err	file	/var/log/no_facility.log	
Platform	err	file	/var/log/Platform.log	
SettingsManager	err	file	/var/log/SettingsManager.log	
sipmmi	err	file	/var/log/sipmmi.log	
Telephony	err	file	/var/log/Telephony.log	
$level ictaudio debug	//To set the ictaudio log to debug level			
$voicemode	//To check current voice mode.			
$rtp 0	//To check current rtp status			
$rtp 1	//To check current rtp status			

8.8 Collecting dbus messages

The dbus messages deal with communications between different applications (processes) in the phone.

Export the dbus messages into a file as below, and download this file for ALE International analysis.

```
$cd /tmp/                    //To save the dbus messages into a file.

$dbus-monitor > /tmp/dbuslog
```

8.9 Collecting trace after MMI issue

For MMI issues, it is better to record a video for better understanding.

To collect the trace for MMI:

$ level	//To show the trace level			
ACTIVITY	LEVEL	SUPPORT	DESTINATION	
ApplicationManager	err	file	/var/log/ApplicationManager.log	
ictaudio	err	file	/var/log/ictaudio.log	
ICTCliGateLite	err	file	/var/log/ICTCliGateLite.log	
ictsipua	err	file	/var/log/ictsipua.log	
LoggerModule	err	file	/var/log/LoggerModule.log	
no_facility	err	file	/var/log/no_facility.log	
Platform	err	file	/var/log/Platform.log	
SettingsManager	err	file	/var/log/SettingsManager.log	
sipmmi	err	file	/var/log/sipmmi.log	//location of sipmmi log
Telephony	err	file	/var/log/Telephony.log	
$ level sipmmi debug	//To set the sipmmi log to debug level			

9. Accessing logs

You can retrieve the SIP phone log files from WBM or using a syslog server.

9.1 Accessing logs from the set Web Management

To capture network traces via WBM:

1) Log in to WBM and go to: Maintenance > Log collection
2) Press the Start button to start the network capturing
3) Once the capturing trace is done, press the Download button to save the trace on your PC

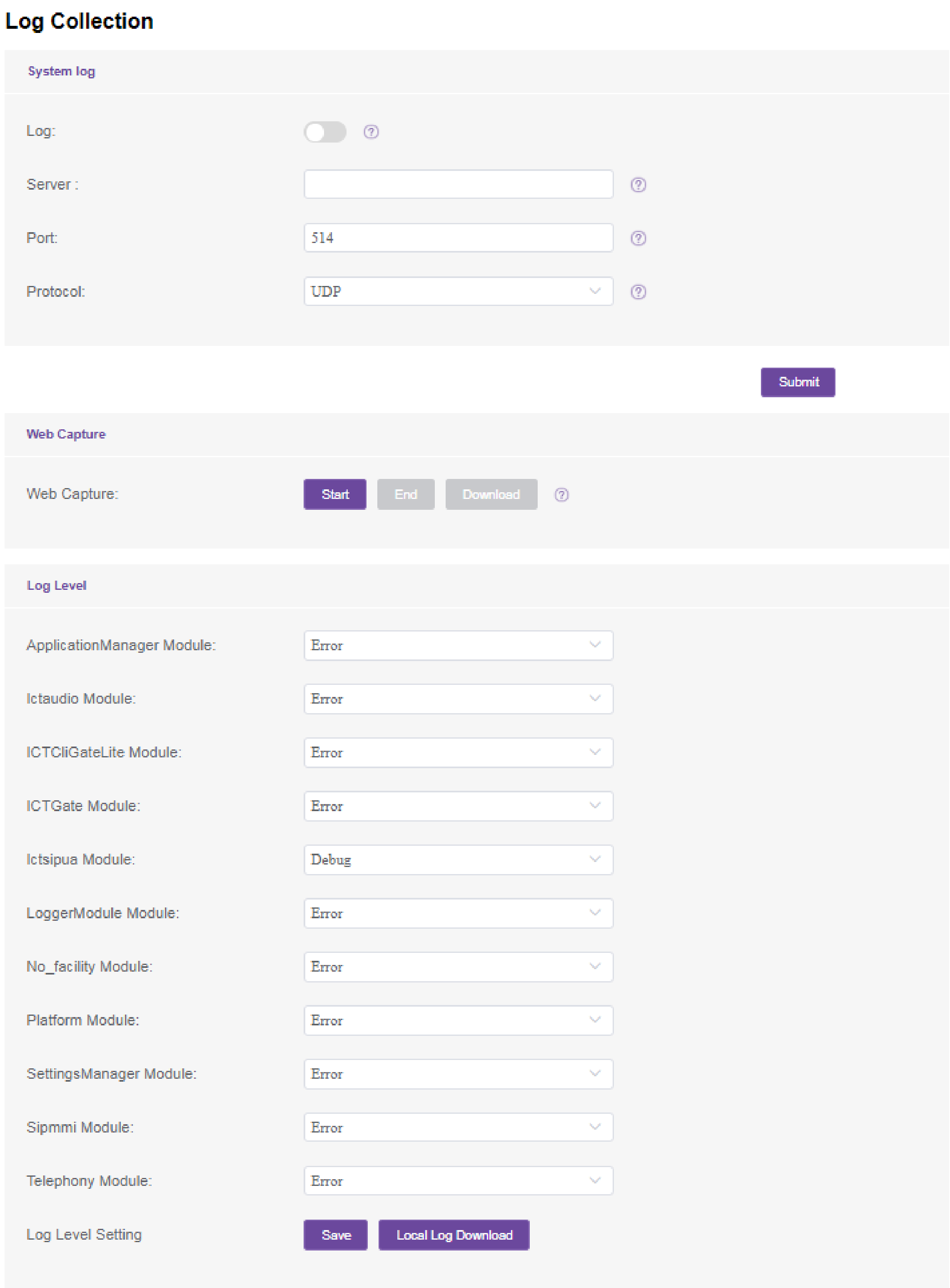
To set the log level and download logs via WBM:

1) Log in to WBM and go to: Maintenance > Log collection
2) Select the trace/log levels for the different facilities and click Save

Note:

The debug level takes more CPU load and memory usage which has an impact on the phone performance. That's why the level should be set to debug only for debug purposes, and should be set back to err when there are no more errors or after all the necessary log information has been captured.

3) Click Download to save traces/logs on your PC



9.2 Accessing logs from a syslog server

To retrieve SIP phone log files using a syslog server:

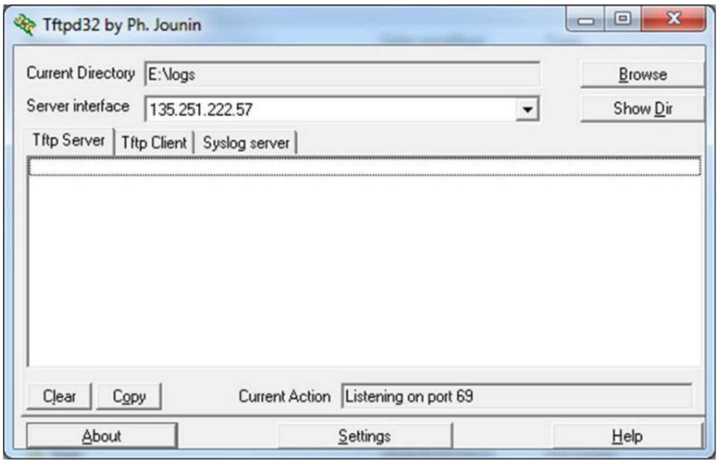
1) Connect to the device under test via SSH and login as admin

2) Use the following command to change all logs with debug level

```
$ level all debug
```

3) Install and start up a syslog server locally

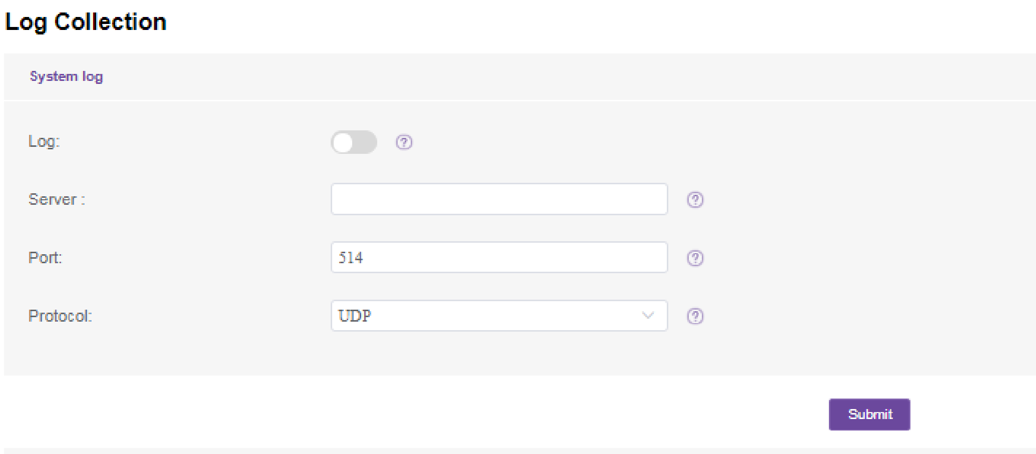
For example:



4) Log in to WBM and go to: Log Collection > Log Collection> System Log

5) Fill in the related contents and press Submit

You will obtain the log files by syslog server.



10. Factory Reset

10.1 Factory reset on the phone

On the Myriad series phone press “Conference” Key for more than 10s, one warning page will pop up. You can press sfotkey to let the phone reset to factory mode.

10.2 Factory reset from MMI

For CE phone to do a factory reset from the MMI:

1) On the phone set, press the navigator right key to display the settings menu

2) Select **Admin** and enter the password (password by default:123456)

3) Press the navigator down key to display the last page, and select **Restore factory**

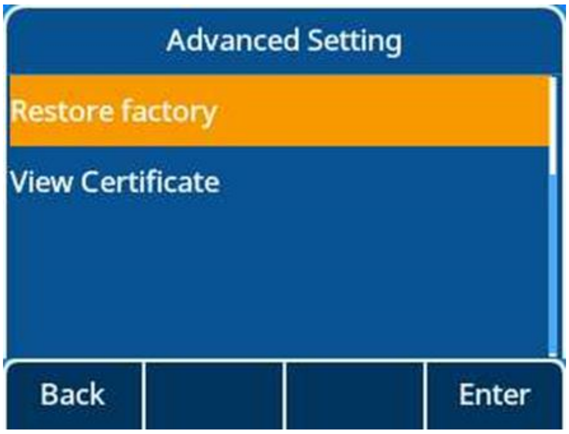
4) Select OK to confirm

For M phone to do a factory reset from the MMI:

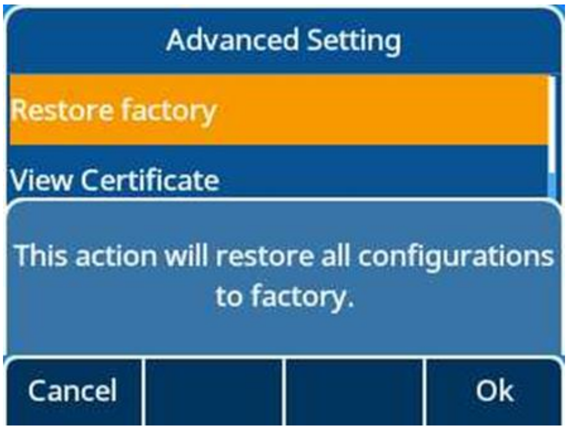
1) On the phone set, press the navigator right key to display menu list

2) Select **Advance Setting** and enter the password (password by default:123456)

3) Press the navigator down key to display the last page, and select **Restore factory**



4) Select **OK** to confirm



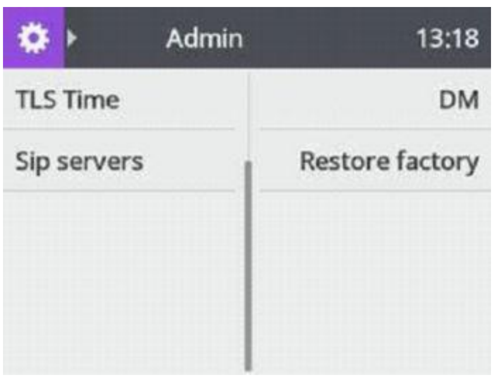
10.3 Factory reset from WBM

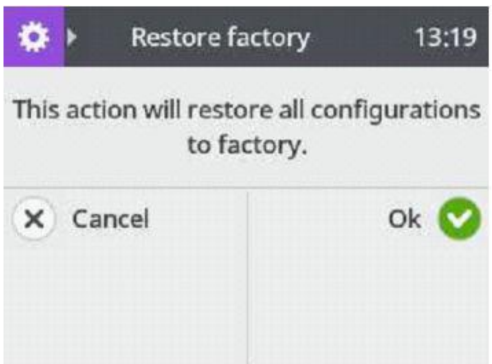
To do a factory reset from the phone web based interface:

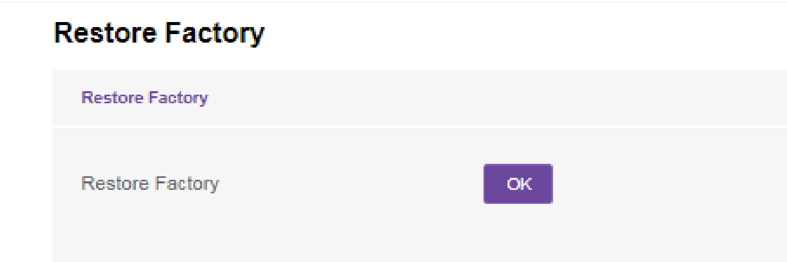
1) Log in to WBM and go to: **Maintenance** > **Restore factory**

2) Click **Restore factory**

The phone restarts with all parameters restored to their factory values: this includes IP parameters and the set restarts in dynamic mode






Restore Factory
Restore Factory
Restore Factory
OK

11. Appendixes

11.1 SIP configuration file templates

The configuration file must be named as config.xxxxxxxxxxxx.xml, and xxxxxxxxxxxx is the mac address of the phone.

Note: Only Account1 configuration template involved in the following template, you can extend it to another 5 accounts as ALE M series phone support 6 accounts.

```
<?xml version="1.0" encoding="UTF-8" ?>
<settings>

    Account1 setting
    <setting id="SIPGroup1AuthenticationName" value="" override="true"/>
    <setting id="SIPGroup1AuthenticationPassword" value="" override="true"/>
    <setting id="SIPGroup1DeviceUri" value="" override="true"/>
    <setting id="SIPGroup1DisplayName" value="" override="true"/>
    <setting id="SIPServer1Address" value=""  override="true"/>
    <setting id="SIPGroup1DtmfMode" value="2" override="true"/>
    <setting id="SIPGroup1LabelName" value="" override="true"/>
    <setting id="SIPGroup1SessionTimer" value="0" override="true"/>
    <setting id="SIPGroup1SessionTimerRefresher" value="0" override="true"/>
    <setting id="SIPGroup1SIPsURIUsage" value="false" override="true"/>
    <setting id="SIPGroup1SrtpWorkingMode" value="0" override="true"/>
    <setting id="SIPGroup1TLSAnticipation" value="false" override="true"/>
    <setting id="SIPGroup1TransportMode" value="0" override="true"/>
    <setting id="SIPGroup1ServerType" value="0" override="true"/>
    <setting id="SIPServer1GenericPollingTimer" value="40" override="true"/>
    <setting id="SIPServer1GroupNumber" value="1" override="true"/>
    <setting id="SIPServer1KeepAliveEnable" value="true" override="true"/>
    <setting id="SIPServer1Port" value="5060" override="true"/>
    <setting id="SIPServer1RegisterExpire" value="120" override="true"/>
    <setting id="SIPServer1SubScribleExpire" value="3600" override="true"/>
    <setting id="SIPServer1FailoverAddress" value="" override="true"/>
 <setting id="SIPServer1FailoverPort" value="5060" override="true"/>
 <setting id="SIPServer1FailoverRegisterExpire" value="3600" override="true"/>
```



```
<setting id="SIPServer1SwitchoverTimer" value="60" override="true"/>
<setting id="SIPGroup1OutBoundProxyAddress" value="" override="true"/>
<setting id="SIPGroup1OutBoundProxyPort" value="5060" override="true"/>
        <setting id="SipUserPhoneEnable1" value="true" override="true"/>

        Account2 setting
        <setting id="SIPGroup2AuthenticationName" value="" override="true"/>
        <setting id="SIPGroup2AuthenticationPassword" value="" override="true"/>
        <setting id="SIPGroup2DeviceUri" value="" override="true"/>
        <setting id="SIPGroup2DisplayName" value="" override="true"/>
        <setting id="SIPGroup2DomainName" value="" override="true"/>
        <setting id="SIPGroup2DtmfMode" value="2" override="true"/>
        <setting id="SIPGroup2LabelName" value="" override="true"/>
        <setting id="SIPGroup2SessionTimer" value="0" override="true"/>
        <setting id="SIPGroup2SessionTimerRefresher" value="0" override="true"/>
        <setting id="SIPGroup2SIPsURIUsage" value="false" override="true"/>
        <setting id="SIPGroup2SrtpWorkingMode" value="0" override="true"/>
        <setting id="SIPGroup2TLSAnticipation" value="false" override="true"/>
        <setting id="SIPGroup2TransportMode" value="0" override="true"/>
        <setting id="SIPGroup2ServerType" value="10" override="true"/>
        <setting id="SIPServe2Address" value="" override="true"/>
        <setting id="SIPServer2GenericPollingTimer" value="40" override="true"/>
        <setting id="SIPServer2GroupNumber" value="1" override="true"/>
        <setting id="SIPServer2KeepAliveEnable" value="true" override="true"/>
        <setting id="SIPServer2Port" value="5060" override="true"/>
        <setting id="SIPServer2RegisterExpire" value="120" override="true"/>
        <setting id="SIPServer2SubScribleExpire" value="3600" override="true"/>
        <setting id="SIPServer2FailoverAddress" value="" override="true"/>
<setting id="SIPServer2FailoverPort" value="5060" override="true"/>
<setting id="SIPServer2FailoverRegisterExpire" value="3600" override="true"/>
<setting id="SIPServer2SwitchoverTimer" value="60" override="true"/>
<setting id="SIPGroup2OutBoundProxyAddress" value="" override="true"/>
<setting id="SIPGroup2OutBoundProxyPort" value="5060" override="true"/>
```



```
SIP Settings
<setting id="SIPRegisterRetry" value="300" override="true"/>
<setting id="SIPLocalSipPort" value="5060" override="true"/>
<setting id="SIPLocalSipsPort" value="5061" override="true"/>
<setting id="SIPLocalSrtpPort" value="30000" override="true"/>
<setting id="SIPLocalSrtcpPort" value="30001" override="true"/>
<setting id="SIPLocalRtpPort" value="6000" override="true"/>
<setting id="SIPLocalRtcpPort" value="6001" override="true"/>
<setting id="SipUserPhoneEnable1" value="true" override="true"/>

Local conference
<setting id="SIPLocalConfEnable1" value="true" override="true"/>
<setting id="SIPMaxCall" value="true" override="true"/>
<setting id="LocalConfPartyMax" value="true" override="true"/>

Rport:
<setting id="SIPServer1RportEnabled" value="false" override="true"/>

Mtu
<setting id="DmEnetcfgInterfaceMtu" value="1200" override="true"/>

Voicemail
<setting id="TelephonyVmNumber1" value="" override="true"/>
<setting id="SIPMessageWaitingIndicationUri1" value="" override="true"/>
Device Management Parameters
<setting id="DmEnetcfgDns1" value="" override="true"/>
<setting id="DmEnetcfgDns2" value="" override="true"/>
<setting id="DmLldpcfgPowerPriority" value="2" override="true"/>
<setting id="DmWpa8021xcfgMode" value="OFF" override="true"/>
<setting id="DmSecucfgPcPort" value="true" override="true"/>
<setting id="DmSecucfgSsh" value="false" override="true"/>
<setting id="DmAdminPasswd" value="123456" override="true"/>

ringing timeout
```


<setting id="RingingTimeout" value="3600" override="true"/>

<setting id="CallIdleTimeout" value="4" override="true"/>

Tone Settings

<setting id="AudioToneCountry" value="8" override="true"/>

<setting id="DialingToneEnabled" value="true" override="true"/>

<setting id="AudioDtmfFeedbackEnable" value="true" override="true"/>

<setting id="AudioDtmfDuration" value="0" override="true"/>

Timezone setting

<setting id="DmAdmcfgTimeZoneUtoffset" value="+1:00" override="true"/>

<setting id="DmAdmcfgTimeZoneLocation" value="Paris" override="true"/>

<setting id="DmAdmcfgDstEnable" value="2" override="true"/>

<setting id="DmEnetcfgSntp" value="0.pool.ntp.org" override="true"/>

<setting id="DmEnetcfgSntpRefreshPeriod" value="3600" override="true"/>

Language Setting

<setting id="language" value="0" override="true"/>

Firmware Upgrading

<setting id="DmEnetcfgUpgradeFile" value="" override="true"/>

<setting id="DmAdmcfgUpdateTimeEnable" value="true" override="true"/>

<setting id="DmAdmcfgUpdateTimeStart" value="03:00" override="true"/>

<setting id="DmAdmcfgUpdateTimeDelta" value="5" override="true"/>

<setting id="DmAdmcfgUpdatePollingEnable" value="true" override="true"/>

<setting id="DmAdmcfgUpdatePollingTimeout" value="3600" override="true"/>

Polling and Update cfg

<setting id="CfgfilePollingByWeekDaysEnable" value="true" override="true"/>

<setting id="CfgfilePollingBeginTime" value="03:00" override="true"/>

<setting id="CfgfilePollingEndTime" value="04:00" override="true"/>

<setting id="CfgfilePollingDayofWeek" value="0123456" override="true"/>

<setting id="DmAdmcfgCfgfilePollingEnable" value="true" override="true"/>

peer to peer

```
<setting id="SipPeerToPeerEnabled" value="true" override="true"/>
```

codec

```
<setting id="SIPPreferredVocoder1" value="8;0;9;18;98;125" override="true"/>


<setting id="OpusBandwidth" value="1" override="true"/>
<setting id="iLBCFrameMode" value="30" override="true"/>
```

Audio SIP

```
<setting id="AudioPayloadTypes1" value="101;96" override="true"/>
<setting id="AudioVad1" value="false" override="true"/>
<setting id="AudioPacketTime1" value="20;20;20;20;20;20" override="true"/>
```

Auto Answer

```
<setting id="TelephonyInterphonyStatus1" value="false" override="true"/>
```

Intercom

```
<setting id="SIPAutoAnsweredAllowed1" value="true" override="true"/>
<setting id="SIPAutoAnsweredMute1" value="false" override="true"/>
<setting id="SIPAutoAnsweredTone1" value="true" override="true"/>
<setting id="SIPAutoAnsweredBarge1" value="false" override="true"/>
<setting id="SIPGroup1IntercomType" value="0" override="true"/>
<setting id="IntercomAutoAnswer" value="false" override="true"/>
<setting id="IntercomCallInfo" value="false" override="true"/>
```

dailing Rule

```
<setting id="DialingRuleEnableHistory1" value="false" override="true"/>
<setting id="DialingRuleEnableContact1" value="true" override="true"/>
<setting id="DialingRuleEnableForward1" value="false" override="true"/>
<setting id="DialingRuleEnableManual1" value="false" override="true"/>
<setting id="Server1DialingRuleCountryCode" value="" override="true"/>
<setting id="Server1DialingRuleAreaCode" value="" override="true"/>
<setting id="Server1DialingRuleExternalPrefix" value="" override="true"/>
<setting id="Server1DialingRuleMinNumberLength" value="" override="true"/>
<setting id="Server1DialingRuleExternalPrefixExceptions" value="" override="true"/>
```

Forward setting

```
<setting id="ForwardModeAccount" value="0" override="true"/>
<setting id="TelephonyFwdMethod" value="0" override="true"/>
<setting id="ForwardImmState" value="false" override="true"/>
<setting id="ForwardImmDest" value="" override="true"/>
<setting id="ForwardImmOnCode" value="" override="true"/>
```

```
<setting id="ForwardImmOffCode" value="" override="true"/>
<setting id="ForwardBusyState" value="false" override="true"/>
<setting id="ForwardBusyDest" value="" override="true"/>
<setting id="ForwardBusyOnCode" value="" override="true"/>
<setting id="ForwardBusyOffCode" value="" override="true"/>
<setting id="ForwardNoReplyState" value="false" override="true"/>
<setting id="ForwardNoReplyDest" value="" override="true"/>
<setting id="ForwardNoReplyOnCode" value="" override="true"/>
<setting id="ForwardNoReplyOffCode" value="" override="true"/>
```

DND setting

```
<setting id="DndModeAccount" value="0" override="true"/>
<setting id="TelephonyDndMethod" value="0" override="true"/>
<setting id="TelephonyDndState" value="" override="true"/>
<setting id="TelephonyDndOnCode" value="" override="true"/>
<setting id="TelephonyDndOffCode" value="" override="true"/>
```

Program Key

```
<setting id="PhoneProgKey1Type" value="" override="true"/>
<setting id="PhoneProgKey1Account" value="" override="true"/>
<setting id="PhoneProgKey1Label" value="" override="true"/>
<setting id="PhoneProgKey1Number" value="" override="true"/>
<setting id="PhoneProgKey1Extension" value="" override="true"/>
```

LDAP

```
<setting id="LDAPEnabled" value="true" override="true"/>
<setting id="LDAPFieldsMapping" value="{ &quot;firstname&quot; : &quot;givenname&quot;, &quot;name&quot; : &quot;sn&quot;, &quot;officephone&quot; : &quot;telephonenumber&quot;}" override="true"/>
<setting id="LDAPLogin" define="default" override="true"/>
<setting id="LDAPPassword" define="default" override="true"/>
<setting id="LDAPServerUrl" value="" override="true"/>
<setting id="LDAPFilter" value="(|(givenname=*%1*)(sn=*%1*))" override="true"/>
<setting id="LDAPSearchBase" value="o=ALE,o=directoryRoot" override="true"/>
```

Phonebook:


```xml
<setting id="PhonebookUrl" value="" override="true"/>



</settings>
```


11.2 Description of the SIP Settings in configuration file

Sections below give a description for the main SIP settings in configuration file. The list of settings is not exhaustive.

11.2.1 Firmware upgrading

Parameter	Default	Value range	Mandatory	Description
DmEnetcfgUpgradeFile			N	Downloading URL for firmware binary files
DmAdmcfgUpdateTimeEnable	false	true; false	N	True: the phone will check the binary version. If different from current version, the upgrading process will be triggered. False: phone will not check the binary information any more.
DmAdmcfgUpdateTimeStart	00:00		N	Defines when the phone will check if the binary has changed during the last 24 hours. Time format supported: HH:MM
DmAdmcfgUpdateTimeDelta	0	[0,1440]		In order to prevent all terminals from starting upgrade at the same time, this setting will add a random value between 0 and 1440 min before the value defined with DmAdmcfgUpdateTimeStart. In this way, upgrade parameters can be configured with the same values for all sets, but each sets will update at different time.

11.2.2 SIP Servers/Groups/Accounts

Note:

SIP Group1/Server1 is mandatory for the main SIP Server (other groups are not described in this document)

Parameter	Default	Value range	Mandatory	Description
SIPServer1Address			Y	SIP Server1 address
SIPServer1Port	5060	0-65535	N	SIP Server1 port number for registration
SIPServer1GroupNumber	1	[0,1440]	N	Group number of this SIP Server1

Parameter	Default	Value range	Mandatory	Description
SIPGroup1ServerType	0	0:Default 4:swyx 5:uaCSTA 6:BroadSoft 7:Asterisk	N	Server type for group1 *Note:* *DO NOT USE 1,2,3 which* *areALEInternational* *solutions*

		8:3cx 9:SIPWISE 10.MetaSwitch		
SIPGroup1DomainName			N	Group1 SIP Server Domain Name
SIPGroup1AuthenticationRealm			N	Group1 SIP Authentication Realm
SIPGroup1AuthenticationName			N	Group1 SIP authenticate name. Mandatory if SIP Server requests authentication
SIPGroup1AuthenticationPassword			N	Group1 SIP authenticate password Mandatory if SIP Server requests authentication
SIPGroup1DisplayName			N	Group1's display name
SIPGroup1DtmfMode	2	0:None 1:InBand 2:RFC2833 3:RFC4733 4:SIP_INFO 5:SIP_INFO +RFC2833		Defines the DTMF mode
SIPGroup1DeviceUri			Y	Group1's device URL used to register

11.2.3 Outbound proxy

In some network topologies, outbound proxy will be used for sip registration. Below are the related

Parameter	Default	Value range	Mandatory	Description
SIPGroup1OutBoundProxyAddress			N	Outbound Proxy Address for group1
SIPGroup1OutBoundProxyPort	5060	0-65535	N	Outbound Proxy port for group1

parameters to be used in the case.

11.2.4 SIP-TLS/SRTP

To deploy the phone to be working in SIP-TLS & SRTP mode, below parameters should be configured in that sip Group.

Parameter	Default	Value range	Mandatory	Description
SIPGroup1TransportMode	0	0:UDP 1:TCP 2:TLS 3:DNS NAPTR	N	Protocol used on transport layer for server group1 Note: If select “3:DNS NAPTR” and then set up port as “0”, the phone will enable NAPTR/SRV.
SIPGroup1SrtpWorkingMode	0	0:none 1:Best effort 2:Strict	N	SRTP mode used on transport layer for server group1

11.2.5 Management of SSL Connection

Parameter	Default	Value range	Mandatory	Description
DmSecucfgSsh	false	true false	N	Enables ssh connections
DmAdminPasswd			N	used to set password for the user **admin**

11.2.6 SNTP & Timezone

Parameter	Default	Value range	Mandatory	Description
DmEnetcfgSntp			N	SNTP Server
DmAdmcfgTimeZoneUtoffset		-11:00 -10:00 -9:30 -9:00 -8:00 -7:00 -6:00 -5:00 -4:30 -4:00 -3:30 -3:00 -2:30 -2:00 -1:00 0 +1:00 +2:00 +3:00 +3:30 +4:00 +4:30 +5:00 +5:30 +5:45 +6:00 +6:30 +7:00 +8:00 +8:45 +9:00 +9:30 +10:00 +10:30 +11:00 +11:30		offset time from UTC time

		+12:00 +12:45 +13:00 +13:30 +14:00		
DmAdmcfgTimeZoneLocation				country or area name of time zone, useful when DST enable is auto
DmAdmcfgDstEnable	0	0,1		0 is diable, 1 is enable
DmAdmcfgDstType	week	Week date		DST is set by week or by date
DmAdmcfgDstStartMonth	Jan	Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec		
DmAdmcfgDstStartWeek	5	1,2,3,4,5		1 is first, 2 is second, 3 is third, 4 is fourth, 5 is last
DmAdmcfgDstStartDate	1			
DmAdmcfgDstStartHour	0	[0.23]		
DmAdmcfgDstEndMonth	Dec	Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec		
DmAdmcfgDstEndWeek	5	1,2,3,4,5		1 is first, 2 is second, 3 is third, 4 is fourth, 5 is last
DmAdmcfgDstEndDate	30			
DmAdmcfgDstEndHour	23	[0,23]		
DmAdmcfgDstOffset	60	[-300,300]		offset time when DST is on, in minutes

11.2.7 Customized Logo of Screensaver

Parameter	Default	Value range	Mandatory	Description
ScreensaverLogoURL			N	URL for download the customized logo of screen saver. Note: Only for CE phone.

11.2.8 LDAP

Parameter	Default	Value range	Mandatory	Description
LDAPEnabled	False		N	Enables LDAP function

LDAPServerUri			N	LDAP Server URL Example: ldap://192.168.2.10:389
LDAPSearchBase	o=Alcatel,o=directoryRoot		N	LDAP Search Base Example: o=Alcatel,o=directoryRoot
LDAPFilter	(|(givenName=*%1*) (sn=*%1*))		N	LDAP Fields Mapping Example: (|(givenName=*%1*)(sn=*%1*))
LDAPFieldsMapping	{"firstname": "givenname","name":"sn","officephone":"telephonenumber"}			Example: {"firstname":" givenname", "name":"sn"," officephone":"telephonenumber "}

11.2.9 Phonebook URL

Parameter	Default	Value range	Mandatory	Description
PhonebookUrl			N	Config phonebook url.

11.2.10 Program Key for CE

Parameter	Default	Value range	Mandatory	Description
PhoneProgKey[1,10]Type	0	0: N/A 23:Account 1: SpeedDial 59: BLF 2: BLF List 17:Call Park 22:Retrieve Park 19: XML Browser 21: Intercom 24:Private Hold	N	The type of phone program key
PhoneProgKey[1,10]Account	1		N	The account index of phone program key. 1: Account 1 2: Account 2

				3: Account 3 4: Account 4
PhoneProgKey[1,10]Label			N	The label of phone program key
PhoneProgKey[1,10]Number			N	The number of phone program key
PhoneProgKey[1,10]Extension			N	The extension of phone program key

11.2.11 Program Key on Add on Module for CE

Parameter	Default	Value range	Mandatory	Description
AomProgKey[1,120]Type	0	0: N/A 1: SpeedDial 59: BLF 2: BLF List	N	The type of AOM phone program key
AomProgKey[1,120]Account	1	1: Account 1 2: Account 2 3: Account 3 4: Account 4	N	The account index of AOM phone program key. 1: Account 1 2: Account 2 3: Account 3 4: Account 4
AomProgKey[1,120]Label			N	The label of AOM phone program key
AomProgKey[1,120]Number			N	The number of AOM phone program key
AomProgKey[1,120]Extension			N	The extension of AOM phone program key

11.2.12 Program Key for Myriad Phone

Parameter	Default	Value range	Mandatory	Description
PhoneProgKey[1,28]Type	0	0 - Not Used 1 - Speed Dial 59 - BLF 2 - BLF List 3 - Do Not Disturb 4 - Directory 5 - VoiceMail 6 - Conference 7 - Forward 8 - Transfer	N	The type of phone program key

		9 - Group Listening 10 - HeadSet 11 - Hot Desking 12 - Phone Lock 13 - Prefix 14 - DTMF 15 - Direct Pickup 16 - Group Pickup 17 - Call Park 18 - Recall 19 - XML Browser 21 - Intercom 23 - AudioHub 58 - Hold 60 - Account		
PhoneProgKey[1,28]Account	1	1-8	N	The account index of phone program key. 1: Account 1 2: Account 2 3: Account 3 4: Account 4 5: Account 5 6: Account 6 7: Account 7 8: Account 8
PhoneProgKey[1,28]Label			N	The label of phone program key
PhoneProgKey[1,28]Number			N	The number of phone program key
PhoneProgKey[1,28]Extension			N	The extension of phone program key

